学校编码：10384　　分类号_____密级_____
学号：X2013231046　　UDC _____

厦门大学

工 程 硕 士 学 位 论 文

某市劳动保障网网络安全体系的设计与实施

Design and Implementation of Network Security System for a City's Labor Security Network

李多

指 导 教 师： 王 备 战 教 授
专 业 名 称： 软 件 工 程
论文提交日期： 2015 年 10 月
论文答辩日期： 2015 年 11 月
学位授予日期： 2015 年 12 月

指 导 教 师：_____
答辩委员会主席：_____

2015 年 10 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　月　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（ √ ）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘　要

本文以某市劳动保障网网络安全体系为研究对象，基于 SSL 技术和 PKI 安全体系，为某市劳动保障中心应用系统建立起完善的安全保障机制，保证某市劳动保障中心当前以及今后信息系统的安全。整体安全体系提供以下安全机制：身份合法性、信息保密性、信息完整性、传输安全性。本文首先简要说明了某市劳动保障网安全的现状，指出了某市劳动保障网中存在的问题，同时也简要的说明了本文的研究内容。随后进行了非常详细的功能需求分析，包括安全需求、开通网上业务的需求、SSL 安全网管、扩展应用的安全需求、以及系统网络设计的需求。根据以上需求，对系统进行总体及各个部分的设计。通过对各项功能的叙述及流程图来说明实现的过程，完成该课题的研究。最后，对实现的过程进行测试，测试说明这个课题能够正常应用，基本完成某市劳动保障网网络体系的要求。

通过本项目的顺利实施，为某市的企业单位及个人提供先进的、安全的、方便实用的网上办事服务功能，从而推进某市劳动保障信息化的建设水平，整体提高劳动保障的工作效率与形象，最终建成全市统一、规范、完善的安全网上服务应用系统平台。

某市劳动保障网网络安全服务项目的实施与开展意义重大：一是提高某市信息化建设水平，共同构建“数字某市”；二是方便企业单位及个人使用网上办事服务功能，做到“足不出户”办理相关手续；三是缓解劳动保障传统业务窗口的压力强度，提高整体工作效率与形象。

关键词：劳动保障；信息系统安全；信息化

Abstact

In this dissertation, we use the network security system of a city municipal labor security system as the research object, based on the SSL technology and PKI security system, to establish a sound security mechanism for the application system of a city labor and social security center, and to ensure that the city labor and social security center as well as the future information system. Overall security system provides the following security mechanisms: identity, information confidentiality, information integrity, transmission security. This paper briefly explains the current situation of the labor security network security in a city, and points out the problems in the work of a city.Then it analyzes the functional requirements of very detailed, including security requirements, online business needs, SSL, security requirements, security network management extension application and system network design requirements According to the above requirements, it makes the overall design of the system and the various parts of the system. Through the description of the various functions and flow chart to illustrate the process to achieve the research. Finally, the process of the implementation of the test, the test shows that the subject can be applied, the basic completion of the work of a city labor and social security network system requirements.

Through the smooth implementation of the project, we can provide the enterprise units and individuals with advanced, safe, convenient and practical functions of the Internet service, so as to promote the construction level of labor and social security in a city and improve the work efficiency and image, and ultimately build the city's unified, standardized, perfect security service application system platform.

And development of the implementation of the city Municipal Labor and social security network security services is of great significance: First, it is improve the construction level of city information, Co Construction of "digital city". Second, to facilitate business units and individuals using online services, do "homes" for the relevant formalities. Third, it is to alleviate the labor protection of traditional business window on the intensity of pressure, improve the overall work efficiency and image.

Key words: Labor Security; Information System Security; Information Technology

目录

第一章 绪论.....1

1.1 研究基础和研究意义.....1

1.2 国内外研究现状.....2

1.2.1 国外研究现状.....2

1.2.2 国内研究现状.....3

1.3 主要研究内容及特色.....4

1.4 本课题的逻辑组织结构.....5

第二章 网络安全体系的需求分析.....6

2.1 某市安全现状.....6

2.2 系统存在的安全隐患.....7

2.3 安全需求.....8

2.3.1 定点机构身份合法性认证.....8

2.3.2 劳动保障所社区身份合法性认证.....8

2.3.3 企业身份合法性认证.....8

2.3.4 数据传输安全性保障.....8

2.3.5 信息的可靠性、真实性保证.....8

2.3.6SSL 安全网关.....9

2.3.7 扩展应用的安全需求.....9

2.4 用户需求.....9

2.5 功能的需求.....10

2.5.1 开通网上业务的需求.....10

2.5.2 系统网络设计需求.....10

2.6 本章小结.....11

第三章 网络安全体系的设计.....12

3.1 设计原则.....12

3.2 系统总体结构设计.....13

3.3 系统应用结构.....18

3.3.1 系统结构设计 19
3.4 安全保障设计 20
3.5 系统功能设计 21
3.6 本章小结 25
第四章 安全体系的实施与测试 26
4.1 证书管理系统 26
4.1.1 证书管理系统建设的必要性 26
4.1.2 “应需而变”的证书管理系统优势 27
4.2 证书服务流程实现 28
4.3 应用安全接入 32
4.3.1 安全接入逻辑结构 33
4.3.2 网络结构 33
4.3.3 安全接入网关 35
4.4 安全认证客户端 35
4.4.1 安全接入实现 35
4.4.2 客户端认证流程 36
4.5 VPN 专线测试 37
4.5.1 VPN 专线测试范围 37
4.5.2 VPN 专线接入流程 37
4.5.3 VPN 专线测试过程 38
4.5.4 VPN 专线测试结果 43
4.6 SSL 安全认证网关压力测试 43
4.6.1 测试范围 43
4.6.2 准备工作 43
4.6.3 测试过程 44
4.6.4 测试结果分析及结论 44
4.7 SSL 安全认证网关稳定性测试 55
4.7.1 测试范围 55
4.7.2 准备工作 55

4.7.3 测试过程 55
4.7.4 测试结论 56
4.8 本章小结 56
第五章 总结与展望 **57**
5.1 总结 57
5.2 展望 57
参考文献 **59**
致谢 **61**

Contents

Chapter 1 Introduction 1

1.1Research Basis and Research Significance 1

1.2 Domestic and International 2

1.2.1International 2

1.2.2Domestic 3

1.3Main Research Contents and Characteristics 4

1.4Organization Structure of the Dissertation 5

Chapter 2 Network Security System Requirements Analysis 6

2.1Safe Present Situation of a City 6

2.2 Security Risks in The System 7

2.3 Security Requirement 8

2.3.1The Legal Identity of The Designated Institutions Certification 8

2.3.2Community Identity Authentication of Labor Security 8

2.3.3Enterprise Identity Authentication 8

2.3.4 The Security of Data Transmission 8

2.3.5 Reliability and Authenticity of Information 8

2.3.6 SSL Security Gateway 9

2.3.7Security Requirements of Extended Application 9

2.4User Damand 9

2.5Functional Requirement 10

2.5.1 Demand for Online Business 10

2.5.2 Design Requirements of System Network 10

2.6 Summary 11

Chapter 3 Network Security System Design 12

3.1 The Design Principle 12

3.2 TheDesign of The System Overall Logical Structure 13

3.3 System Application Logic Structure 18

3.3.1 System Structure Design 19
3.4 Security Design 20
3.5 System Function Design 21
3.6 Summary 25
Chapter 4 Security System Implementation and Test 26
4.1 Certificate Management System 26
4.1.1 The Necessity of The Construction of Certificate Management System 26
4.1.2 The Advantage of The “Change with Demand”Certificate Management System 27
4.2 Certificate Service Process implementation 28
4.3 The Application of Security Access 32
4.3.1 Secure Access Logic Structure 33
4.3.2 Network Structure 33
4.3.3 Secure Access Gateway 35
4.4 Security Authentication Client 35
4.4.1 Implementation of Security Access 35
4.4.2 Client Authentication Process 36
4.5 VPN Dedicated Line Test 37
4.5.1 VPN Test Range 37
4.5.2 VPN Access Process 37
4.5.3 VPN Line Test Procedure 38
4.5.4 VPN Dedicated Line Test Results 43
4.6 SSL Security Authentication Gateway Pressure Test 43
4.6.1 Test Range 43
4.6.2 Preparation 43
4.6.3 Test Procedure 44
4.6.4 Test Result Analysis and Conclusion 44
4.7 SSL Security Authentication Gateway Stability Test 55

4.7.1 Test Range 55
4.7.2 Preparation 55
4.7.3 Preparation 55
4.7.4 Test Conclusion 56
4.8 Summary 56

Chapter 5 Conclusions and Outlook 57

5.1 Conclusions 57
5.2 Outlook 57

References 59

Acknowlegements 61

第一章 绪论

1.1 研究基础和研究意义

某市社会保险管理信息系统建设，是以劳动和社会保障部推出的社会保险核心平台及劳动保障就业两个系统为核心，充分借鉴和吸取国外和国内其他地区的一些先进经验，并在此基础上建设的。经过多年的努力，系统建设取得了最初的成绩，核心平台综合业务、养老保险和失业保险的缴费及支付、医疗保险结算等子系统已逐步进入运行阶段。我们按照劳动和社会保障部的要求，统一和规范了社会保险经办业务的操作，市本级社会保险经办业务已全面应用计算机信息系统管理，整个指标体系完全符合国家劳动保障部指标要求并有所扩展，建立了市本级基础资源数据库（生产区），目前社会保险信息系统、劳动就业系统已延伸到某市的十个区县市劳动保障经办机构及劳动保障所、社区，医疗保险已联接定点医疗机构 178 家，定点零售药店 188 家，系统 24 小时不间断运行，并开展了网上劳动保障查询业务。 2006 年劳动保障业务涵盖了企业养老保险 36.68 万人、失业保险 20.15 万人、医疗保险 55.82 万人、工伤保险 45.77 万人、生育保险 41.29 万人及 12.07 万人机关事业单位的医疗保险业务。劳动保障工作正全面向数字化迈进。数字系统在社会劳动保障工作中正发挥着日趋重要的作用。现在，我们将社会保险系统与就业服务系统延伸到区、县（市）和社区、劳动保障所，实现数据大集中，分级管理模式[1]。

为了运用信息技术向社会普及劳动保障知识，广泛宣传劳动保障法律、法规、政策及业务流程，以快速、便捷的方式向市民提供咨询服务，我们开展了基于 Web 的某市劳动保障电话咨询服务中心的建设（劳动保障 12333 咨询服务中心）。该系统的建设是基于就业服务信息系统和社会保险管理信息系统为基础进行的，系统的规划和建设具有一定的超前性，满足国家劳动保障部《关于开展劳动保障电话咨询服务的通知》要求。咨询服务中心接入号码“12333”于 2003 年 7 月 28 日正式开通，市民咨询问题主要集中在下岗再就业优惠证的发放、社会保险的参保、接续及待遇享受，劳动合同的签订、劳动争议仲裁等热点问题上。同时，西南地区首家提供劳动保障政策及相关数据信息查询的专业网站“劳动保障网”也于当天正式开通运行，这是我们开辟的另一条以互联网传递信息的为民服务的新

渠道。无论何时何地，只要登录 WWW. 12333.NET，即可获得劳动保障方面的最新资讯信息及劳动保障相关政策法规、各类表格下载及信息查询等信息[2]。

1.2 国内外研究现状

1.2.1 国外研究现状

1、法国：失业保险、补充养老金

根据法国的相关规定，开发新技术的一个条件就是由失业保险信息体系一体化的两个主要申请形式。因特网技术在里面(20,000 个工作站)和外面同时被应用，这就方便了企业可以通过多个平台获取失业者的信息和求职者也可以最多的获得需要聘用人员的企业信息。这个信息平台使企业可以直接为求职人员提供需要的信息。补充养老保险通过计算机技术得以实现，这样的技术还在不断完善发展，而且已经超出了单独使用电脑申报的范畴，还逐渐包含了信息互换。从而创造了新一代的通讯学服务课题，这种服务是具有独特性的，而且具有普遍的得到此服务的硬件设备：例如多种形式的通讯设备、因特网、各种互通的邮件方式。要求相对少数的人员进入到传送和管理数据信息中，得到的信息安全性就明显提高。这种形式使得信息传送的过程更加安全稳妥。因为这些数据不需要用人员输入信息或者传送，由此可以减低人为发生的失误。数据信息用网络的形式，直接把数据的源头传送到接收的地方。

2、比利时：就业信息直接公告

把就业信息向比利时国家社会保障部门发布，失业情况的各项数据信息以网络平台直接的公告。这样的申报方式是比利时社会保障部门全部方案中的一部分，意在缓解行政管理方面规章制度对用人单位的要求。

比利时社会保障部门的这种方式对整个系统体系的影响：

（1）没有书面的各种报告。优点在于避免了人为操作的影响。

（2）使用全新的自动控制系统。优点在于速度得到进一步提高，安全性更强。

（3）用人单位使用表格和数据自动化。优点在于人为操作减少，提高准确度。

（4）全部的功能体现在一个报告里。优点在于减少对一个程序的操作环节。

3、加拿大:就业信息

在加拿大，以因特网技术为根本的许多电子政务平台得到很好的发展应用，

我们主要学习一下就业信息服务方面，信息库把用人单位提供的全部工作机会整整合集中在一个平台，有求职意愿的劳动者，只要登录因特网进入平台就可以得到相关信息。

加拿大政府以本国公民的立场考虑，把数据信息分类集中整合以后，再通过信息平台给劳动者提供 20 个服务项目。劳动保障部门建立的“工作、工人、培训和职业”方案为有求职意愿的劳动者提供了得到工作的机会、技术的培训、以及关于工作的相关资讯、互动的培训和网络学习，并为处于转型期的加拿大公民给予窗口服务项目。方案还向企业提供直接在因特上出具招聘岗位的信息。

1.2.2 国内研究现状

1、广州市人力资源和社会保障部门

从广州市人力资源和社会保障部门获悉，为了不断提升社保业务的办理水平和工作效率，方便市民及各类企业办理劳动保障相关业务，目前广州市劳动保障信息网(www.gzlss.gov.cn)开通了 5 项劳动保障业务，参保单位在该网成功办理的社会保险业务，原则上不再需要提交任何纸质材料给社会保险经办机构，实现足不出户就可以办理社会保险业务。

市劳动和社会保障局有关负责人表示，网上办理劳动保障业务具有申报操作便民高效、数据准确安全等特点。目前可在广州劳动保障信息网上办理的社会保险业务有 5 项，包括新增人员办理参保、减少人员办理停保、单位和个人申报缴费、单位基本信息查询及修改、个人基本信息查询及修改，今后劳动保障部门还会不断扩大业务办理网上实现的范围。

劳保部门特别提醒，为了保证网上办理社会保障业务信息安全、真实、可靠，根据《中华人民共和国电子签名法》的要求，参保的用人单位在劳动保障网上办理社会保险相关业务必须通过数字证书的验证。办理数字证书的方法，可以查阅广州市数字证书管理中心网站(www.gzca.gd.cn)。

此外，为配合广州市政府推出的市民电子邮局服务，广州市信息中心将为参保单位开通免费的电子邮箱服务，广州市社会保险基金管理中心将逐步通过电子邮局发送关于社会保险的缴费信息、社保政策、办事规定、业务通知等信息给参保单位。办理市民电子邮局，可登录广州市市民电子邮局网站(www.gzemail.cn)查询办理。

2、珠海市劳动和社会保障局:

为了推进珠海市劳动保障数字化管理的应用，维护企业用工和雇员的合法权益，为企业用工手续和办理社会保险提供便利，提高工作效率，根据《中华人民共和国电子签名法》，市人力资源和社会保障数据管理中心自己开发研制了新的网络业务办理系统。这个系统第一次引进了数字证书的手段，具有用人单位申报信息安全准确，使用简单效率高等特点，并经珠海市一些用人单位试用，普遍反应使用效果较好。

用人单位可以自己在珠海市电子政务数字证书或者珠海市电子商务数字证书中选择更适合的。办理珠海市 CA 数字证书认证需要填写要求单位的相关申请表格，用人单位办理的人员要持自己的身份证和单位的营业执照副本原件、复印件和组织机构代码证书复印件到珠海市公司办理单位数字证书认证。

通过以上手续办理劳动保障网上申报分别按劳动用工备案和社会保险业务办理开户登记，填写各类申请表格进行审核。

1.3 主要研究内容及特色

根据国内外经济发达地区的成功经验，开展劳动保障网上服务业务，通过网上办理企业单位及个人各类社会保险是大势所趋，是信息社会高速发展的必然结果。在某市，通过开通劳动保障网上服务业务，企业和个人可以通过互联网实现劳动保障业务的网上办理，可以大大缓解当前劳动保障大厅窗口的业务压力，提高服务形象。但在开展网上服务的同时，因为涉及到企业单位及个人的敏感信息及大量数据，关系到广大市民的切身利益，对身份认证、加密传输、防篡改、防抵赖的需求较高、安全问题成为开展劳动保障网上服务的重中之重，不容忽视。也正是因为安全问题，某市的劳动保障在网上办事服务方面一直没有实质的内容和具体的服务功能[3]。

通过结合国内外的先进经验，PKI/CA 技术是解决网上业务安全问题比较成熟的手段，2005 年 4 月 1 日，《电子签名法》在中国正式施行，确立了数字签名的法律地位；2006 年 7 月 18 日，某市数字证书认证中心的正式揭牌成立，填补了某市信息安全基础设施的空白，为本项目的开展奠定了安全基础[4]。

基于以上，“某市劳动保障网网络安全服务项目”通过采用某市数字证书认证

中心签发的数字证书和认证服务及其它配套安全设备与措施来解决安全问题，通过学习省外劳动保障网上服务的成功经验并结合自身系统的特点进行细致的技术调研来进行应用系统的开发，从而面向企业单位和个人提供一套功能完善、方便实用的安全网上服务应用平台。

1.4 本课题的逻辑组织结构

全文分成五章，各章内容组织如下：

第一章主要分析了论文研究的背景以及我国社会保障网络安全体系现状分析，并将本文的研究内容和主要工作进行了说明。

第二章对现有的社会保障业务安全系统进行结构的描述和具体需求进行分析，并提出新型社会保障安全体系的具体需求和预期的功能目标。

第三章中根据需求分析的结果，对社会保障安全体系的总体架构设计以及该系统的运行环境作了图表及文字的叙述。

第四章中我们系统介绍整个某市社会保障安全系统的实施过程，详细描述了在本课题实施之前的实验室模拟测试、实际环境模拟测试和实施之后的验证测试过程。

第五章首先对全文概况性的总结和分析，探讨了存在的问题以及未来的解决方案，同时对社会保障安全体系作了发展的下一阶段简介。